



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/933,995	08/21/2001	Saed G. Younis	010356	7655

23696 7590 08/22/2005

Qualcomm Incorporated
Patents Department
5775 Morehouse Drive
San Diego, CA 92121-1714

EXAMINER

SCHUBERT, KEVIN R

ART UNIT PAPER NUMBER

2137

DATE MAILED: 08/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/933,995

Applicant(s)

YOUNIS, SAED G.

Examiner

Kevin Schubert

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
 - If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
 - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
 - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 22 July 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-13 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-13 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☐ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: _____

DETAILED ACTION

Claims 1-13 have been considered.

Claim Rejections - 35 USC § 102

5 (e) the invention was described in (1) an application for patent, published under section 122(b),
by another filed in the United States before the invention by the applicant for patent or (2) a
patent granted on an application for patent by another filed in the United States before the
invention by the applicant for patent, except that an international application filed under the treaty
10 defined in section 351(a) shall have the effects for purposes of this subsection of an application
filed in the United States only if the international application designated the United States and
was published under Article 21(2) of such treaty in the English language.

Claims 1 and 7-13 are rejected under 35 U.S.C. 102(e) as being anticipated by Hokkanen, PCT
15 International Publication Number WO 99/53621.

As per claims 1 and 9-13, the applicant describes a method for enabling a mobile apparatus for
call processing comprising the following limitations:

- 20 a) encrypting a random number at the mobile apparatus (Page 10, lines 23-27; Page 9, lines 18-
23; Page 9, line 35 to Page 10, line 3);
- b) sending the random number from the mobile apparatus to a charging apparatus (Page 10,
lines 23-27);
- c) encrypting the random number at the charging apparatus (Page 10, lines 23-27; Page 8, lines
15-16);
- 25 d) receiving at the mobile apparatus the encrypted random number from the charging apparatus
(Page 10, lines 23-27);
- e) enabling the mobile apparatus based on a comparison of the encrypted random number at the
mobile apparatus with the encrypted random number received from the charging apparatus (Page 10,
lines 23-27);

Art Unit: 2137

As per claims 7 and 8, the applicant describes the method of claim 1, which is met by Hokkanen (see above), with the following limitation which is also met by Hokkanen:

Wherein the enabling further includes enabling the mobile apparatus while the mobile apparatus is located within a predetermined distance from the charging apparatus that is dedicated to the mobile apparatus (Page 6, lines 26-33);

The mobile phone is enabled to receive or place calls as a cordless phone after authentication has taken place through a random number exchange between the mobile phone and the home base station charging apparatus. However, the mobile phone also has information programmed into its memory which cancels the enablement with the home base station once the mobile phone moves outside the predetermined range of the home base station.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 2 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hokkanen in view of Menezes (Menezes, Oorschot, Vanstone: Handbook of Applied Cryptography, CRC Press Series on Discrete Mathematics and its Applications, CRC Press, 1997, Pages 397-400).

As per claims 2 and 5, the applicant describes the method of claim 1, which is met by Hokkanen (see above), with the following limitation which is met by Menezes:

Wherein the random number is an encrypted system time (Page 399-400);

Art Unit: 2137

Hokkanen describes all the limitations of claim 1, the independent claim. However, Hokkanen does not describe a process for sending an encrypted system time. In paragraph [1028], the applicant describes that a system time may be sent as a time limitation for enablement: "The register may be loaded with the system time whenever the mobile is successfully enabled for call processing. When a call-processing request is received, the mobile may compare the content of the register with the current system time. If the difference is less than a predetermined time period, the time has not expired and the call processing may be allowed. If the predetermined time period has expired, the mobile may be disabled to handle the requested call processing, and may return to idle state" (Applicant: [1028].

Menezes discloses that using an encrypted system time is an effective way to incorporate "time-limited access privileges" (Page 399). The timestamp, which may be cryptographically binded to a message (encrypted), allows for an acceptable window for a message to be received in.

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Menezes with those of Hokkanen and incorporate the use of an encrypted system time to allow enablement only for a certain amount of time for security reasons.

Regarding claim 5, the enabling of the mobile apparatus for a predetermined period of time is the acceptable window as described above.

Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hokkanen in view of Menezes in further view of Moshopoulos, (Moshopoulos, Nikos; Chaniotakis, Eleftherios. A Survey of Cryptography Algorithms- Trends and Products. National Technical University of Athens. 2000. Pages 1-28).

As per claim 3, the applicant describes the method of claim 2, which is met by Hokkanen in view of Menezes (see above), with the following additional limitation which is met by Moshopoulos:

Wherein the encrypted system time is based on Rijndael 128-bit key encryption technique (Page 15);

Art Unit: 2137

Hokkanen in view of Menezes meets all the limitations of claim 2. However, Hokkanen in view of Menezes fails to disclose the use of Rijndael 128-bit key encryption.

Moshopoulos's paper describes a survey of common cryptography algorithms. Moshopoulos also discloses that Rijndael 128-bit key encryption is one of the fastest encryption algorithms (Page 15).

5 It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate the ideas of Moshopoulos with those of Hokkanen in view of Menezes and use Rijndael 128-bit key encryption because it is a fast encryption algorithm.

10 Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hokkanen in view of Moshopoulos.

As per claim 4, the claim is rejected on the same grounds as claim 3 above except for the fact that claim 3 is rejected under Hokkanen in view of Menezes in further view of Moshopoulos and claim 4 is rejected under Hokkanen in view of Moshopoulos.

15

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hokkanen in view of Blow, WO 99/53621.

20 As per claim 6, the applicant describes the method of claim 1, which is met by Hokkanen (see above), with the following limitation which is met by Blow:

Wherein the enabling further includes enabling the mobile apparatus while the mobile apparatus is positioned on the charging apparatus that is dedicated to the mobile apparatus (Blow: Page 5, lines 27-36; Page 1, lines 15-23; Page 4, lines 3 to 11; Fig 1);

25 Hokkanen describes all the limitations of claim 1, the independent claim. However, in Hokkanen's system the enablement of the apparatus takes place through a wireless connection between the mobile apparatus and the home base station charging apparatus. Thus, Hokkanen lacks the limitation that the enablement takes place on the home base station charging apparatus.

Art Unit: 2137

Blow describes a system similar to Hokkanen's system and the applicant's system in which a wireless communication device, such as a "portable telephone" (Page 1, line 16) authenticates an accessory, such as a "battery charger" (Page 1, line 17). In Figure 1, the wireless communication device, or mobile phone, is 100 and the accessory, or charger, is 102. However, in Blow's system the interface 112 can be a wireless interface or a physical interface such as the mobile phone being physically connected to the accessory (Page 4, lines 3 to 11). The authentication which takes place between the mobile phone and the accessory charging unit is similar to that of Hokkanen's and the applicant's (Page 5, lines 27-36).

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Blow with those of Hokkanen and authenticate the mobile phone on the home base station charging unit in the event that a person wants to make or receive a call while the phone is being charged in the home base station.

Response to Arguments

The claim objections have been withdrawn.

Applicant's arguments filed 7/22/05 with respect to claim 1 have been fully considered but they are not persuasive. The applicant argues the rejection in light of the particular embodiment of Hokkanen in which authentication is performed at the home base station, or the charging unit. The examiner did not rely on this embodiment. As disclosed by the examiner in the first office action, Hokkanen teaches that an authentication process for a mobile phone may take place at the charging unit (home base station) or the mobile phone itself. The examiner points the applicant to the following passage:

"It is also possible to act in such a way that the mobile station authenticates the base station. Hereby it sends to the base station both the IMSI and the RAND, in response to which the base station returns the SRES number. The mobile station checks to make sure that the number corresponds with the already stored or recalculated SRES value." (page 10, lines 23-27)

As disclosed throughout the patent, communication between the mobile phone and the charging unit is encrypted using a ciphering key (Ki). Thus, RAND is encrypted using Ki at the mobile phone and sent to

Art Unit: 2137

the charging unit (parts a and b). RAND is encrypted according to a stored protocol to form SRES, and SRES is sent back to the mobile phone (parts c and d). Finally, a comparison of the SRES received with the SRES stored in the memory of the mobile phone authenticates the charging unit for enablement of operation (part e). Hokkanen thus satisfies all the limitations of claim 1.

5

Applicant's arguments with respect to claims 10-12 have been fully considered but they are not persuasive. The applicant argues that "Hokkanen does not teach or even suggest a charging apparatus comprising a receiver or means for receiving a random number from a mobile apparatus, and a transmitter or means for sending the encrypted random number to the mobile unit". The examiner disagrees. Referring to the passage above, a charging apparatus receives a random number (RAND) and sends the encrypted random number (SRES) to the mobile unit.

Applicant's arguments with respect to claims 2 and 5 have been fully considered but they are not persuasive. The applicant argues that the combination of Menezes with Hokkanen is insufficient because it does not rely on the teachings of Menezes. The examiner disagrees. Menezes discloses the idea that a time stamp may serve as a random number for a challenge-response protocol (pages 398-400). Hokkanen discloses a challenge-response protocol with a random number but does not specifically disclose that the random number is a time stamp. Furthermore, there is motivation to utilize a time stamp as a random number because a time stamp can also prevent replay attacks by precluding use of a message past a certain time limit. Incorporating the ideas of Menezes with Hokkanen allows the mobile station to enable the mobile apparatus only if the random number matches the stored random number and is received back in an acceptable predetermined period of time (for example less than thirty seconds after RAND is sent). This increases security in the system by preventing replay attacks.

25

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Art Unit: 2137

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 7:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KS


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER